Published and Copyright (c) 1999 - 2011
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1350 12/16/11

~ Wikipedia SOPA Protest ~ People Are Talking! ~ Understanding SOPA!
~ Banned Game Gets Award ~ Novell Verdict Close! ~ Chrome 15 Is On Top!
~ Facebook Suicide Help! ~ US, Russia Work United ~ Social Media vs Web!

~ WebOS to Open Source! ~ IE Automatic Updates! ~ Twitter Stalking!

-* No Zing to Zynga’s IPO Debut *-
-* Chrome Is The Most Secure Browser! *-
-* Most People Still Don’t Trust Online Info! *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""

If it’s not being deluged with the GOP political bashing of each other, it’s the onslaught of holiday advertisements in an effort to get us to buy, buy, buy! Yes, they say ’tis the season to be jolly, but I haven’t seen it! I guess it’s the holiday commercialization cynicism in me, but the season seems to generate a lot of apathy.

Sure, many people are full of holiday cheer, but rarely do we see those same people at the malls fighting through the crowds and waiting endlessly at checkout lines. But, I do enjoy seeing all of the various holiday lights displayed on houses and other places. People’s imagination as to how they display holiday decorations always amazes me; and I look forward to seeing the lights and other stuff.

So, I guess that we’re left with taking the good with the bad for another couple of weeks, spend an enjoyable holiday with family and friends, and then fight with the crowds and lines to return those unwanted gifts, and then hopefully survive until the new year! And in another year, we do it all over again! Happy Holidays!

Until next time...

=~=~=~=

->In This Week’s Gaming Section - Investors Give ’Farmville’ Maker A Cold Shoulder!
"""""""""""""""""""""""""""""""" Banned Xbox Game Picks Up Prestigious Award in UK!

=~=~=~=

->A-ONE’s Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""

Investors Give ’Farmville’ Maker A Cold Shoulder

As its workers celebrated with hot chocolate and cinnamon buns, Zynga saw its stock dinged on its first day of trading Friday - an unexpected turn of events for a closely watched public debut seen as a precursor to Facebook’s next year.

Zynga Inc., the online game developer behind "FarmVille," ’’Mafia Wars" and other popular time killers on Facebook, raised at least $1 billion in its initial public offering of stock, the largest for a U.S. Internet company since Google’s $1.4 billion IPO in 2004.

But by Friday afternoon, Zynga’s stock fell 50 cents, or 5 percent, to close at $9.50. The stock priced at $10 on Thursday, at the high end of its expected range. It traded as high as $11.50 on Friday before heading into a downward spiral on the Nasdaq Stock Market.

It was far from the eye-popping jump that has been the trend this year for freshly public Internet darlings such as LinkedIn Corp., which saw its stock double on its first trading day.

Zynga’s opening - with a ticker symbol of "ZNGA" - was supposed to be big. After all, unlike many others with IPOs, the company is profitable, with more than 220 million people playing its games on Facebook each month.

What this all means for Facebook’s IPO, expected sometime after April, is hard to say. One thing is clear, though.

"A hot IPO is not guaranteed," said Kathleen Smith, principal of IPO investment advisory firm Renaissance Capital.

Despite the big-name public offerings this year, the IPO market is not in good health. Buyers are skittish and concerned about the high volatility of freshly public stocks, Smith said. Big name or not, investors don’t want to pay sky-high prices for stocks, especially not before a company has proven itself with good earnings reports and analyst ratings.

Seventy percent of the 125 companies that went public this year are now trading below their IPO price, according to Renaissance Capital.

While Friday’s drop doesn’t look good, it’s not devastating for Zynga. Its CEO, Mark Pincus, said the company’s focus is on "delivering great products" that expand audience for social games over the next few years - and not on the next trading day.

"We didn’t have any expectations coming into this whole process," he said in an interview. "We decided to go public a long time ago."

Pincus rang the Nasdaq’s opening bell in San Francisco, a first in the city for a freshly public company. The company’s roughly 1,700 San Francisco employees woke up at the crack of down to celebrate with cinnamon buns and hot cocoa. Zynga also delivered video of the opening ceremony over the Internet to its offices around the world.

Thursday’s pricing gives Zynga a market value of about $7 billion. That’s roughly half of the value of online deals site Groupon, which began

trading in early November. Zynga, though, sold a much bigger chunk of its available shares, 14.3 percent compared with Groupon’s 5.5 percent. It’s an issue of supply and demand - selling more shares means investors don’t have to scramble to get their hands on them.

Wedbush analyst Michael Pachter said stocks trade based on supply and demand on the first day.

In Zynga’s case, he believes the IPO’s underwriters placed more shares with investors who were going to "flip" the stock - that is, buy a hot stock and quickly sell it to make a profit instead of holding on to it for the long run. All that selling tempered the stock’s price, and other nervous investors started selling, too.

Sterne Agee’s Arvind Bhatia said the issue came down to valuation - what people are willing to pay.

"You might like a company but not its valuation," said Bhatia, who took the unusual step of starting coverage of Zynga’s stock before it went public, giving it an "Underperform" rating and a price target of $7.

With its huge player base and a few loyal spenders, Zynga had net income of $90.6 million in 2010, an unusual pre-IPO money-maker in the sector.

Cowen & Co. analyst Doug Creutz, however, initiated coverage Friday with a "Neutral" rating on the stock. Although Zynga is the leader in Facebook gaming, he’s concerned that it won’t be able to grow fast enough to justify its stock price. Growth in Facebook gaming has slowed, and Zynga’s market share has declined from 50 percent to 38 percent of daily active users, he wrote.

He’s also concerned that Zynga’s famously aggressive and hard-charging culture may not be the best field to grow good games in. Others have raised concerns that the focus on deadlines and profits might be squeezing out creativity and talent.

In November, Groupon raised $700 million in its IPO. The granddaddy of all Internet IPOs might happen next year, as Facebook Inc. is expected to raise as much as $10 billion.

Bhatia declined to speculate about what Zynga’s first-day drop might mean for Facebook. But he pointed out that what was a bad year for Zynga was a good year for Facebook. That’s because Facebook stated charging application developers a 30 percent cut of the money they make through its site. That means for every dollar a player spends on "FarmVille" crops, 30 cents goes to Facebook.

"They are in the driver’s seat," Bhatia said of Facebook. The company, he added, is "in class of its own."

Banned Xbox Game Picks Up Prestigious Award in UK

A computer game banned by Xbox for what it perceived to be risquØ content picked up a top award in the UK recently.

The game, which is designed to educate teenagers about sexually transmitted diseases, bagged the prize at the British Academy Children s

Awards, organized by BAFTA, late last month.

Privates, described by its Brit-based developer Size Five Games as "a sex ed shoot- em-up romp," requires the gamer to "lead a teeny-tiny gang of condom-hatted marines as they delve into peoples vaginas and bottoms and blast away at all manner of oozy, shouty monsters."

It was commissioned by the UK s Channel 4 Television as a way of heightening awareness about the dangers of sexually transmitted diseases.

Privates comprises five levels of "bug-busting action" that takes place among "a variety of gorgeous 3D locations, with a fully-voiced comedy script and a nutso soundtrack."

"You never know," the game s blurb says, "you might even learn something handy about your downstairs-department."

Asked at the award ceremony about the response to his game, creator Dan Marshall said, "I get more fan mail about Privates than for anything else. People love it - and are blown away by its audacious nature."

Marshall said he had been hoping to get the game released on the Xbox 360 but when he sent details of it to the gaming platform, it was rejected. "The original design document broke a vast number of Xbox s rules," Marshall said. "I sent a copy to the very nice people at Xbox, who loved it, but decided that the rules needed to hold steady."

Anyone who wants to try it out is in luck though, as Privates is available for download to PCs for free.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Understanding SOPA: The House Debates The Stop Online Piracy Act

Today, the House Judiciary Committee continued to wrestle the Stop Online Piracy Act before the second legislative session came to an abrupt end. The hearing picked up this morning after more than 20 amendments were rejected over the course of yesterday’s controversial 11-hour long markup process, during which legislators hashed out changes to the bill, which is commonly known as SOPA (H.R.3261). If passed as initially proposed, SOPA would broadly expand the U.S. Department of Justice’s power to enforce copyright - and to demand that internet entities like social networks and search engines take an active role in doing so too. For now a vote is delayed until "the earliest practical day that Congress is in session," which could be weeks from now.

In November, some of the biggest companies on the web came out in full force to oppose a proposed anti-piracy bill as it wended its way through Congress. Prior to the congressional hearing on November 16, a consortium

of nine companies that would be affected by the bill (eBay, Twitter, AOL, Google, Facebook, Yahoo, Mozilla, Zynga, and LinkedIn) released an open letter publicly criticizing SOPA . The hearing only featured a single witness against the proposal: Google's policy counsel, Katherine Oyama. (Since SOPA enjoys bipartisan congressional support, the selection of a single dissenting witness for the opposition, while striking, isn't uncustomary.)

Supporters of SOPA predictably include many names in traditional media distribution, like the MPAA, the RIAA, Comcast/NBCUniversal, and Viacom. The war over the controversial bill highlights a growing rift between new forms of online digital media distribution and the old guard of the recording and broadcast industries - and the very real implications this mounting tension has on web users.

Want to know the basics and how you can take a stand for the future of the open web? Read our SOPA FAQ below.

What is SOPA?
SOPA is the Stop Online Piracy Act (H.R.3261), which was introduced to the House in October by a bipartisan group of 12 supporters. SOPA combines two Senate bills: S.968 and S.978.

What would SOPA do?
The bill would set up a system for the U.S. government to enforce copyright. It would grant the U.S. Attorney General and the U.S. Department of Justice the power to take legal action against sites deemed to be violating copyright. SOPA would also grant the government the power to request that search engines (Google and Bing, for example), internet service providers, and social networks like Facebook block access to a site deemed to be in violation of copyright laws.

Currently, the terms of service agreements on most websites solely pertain to individual users when it comes to illegal content. SOPA would extend the burden of responsibility for copyright violation to the companies that deliver web content to users, as decided and ordered by the Department of Justice.

How would SOPA affect web users?
Beyond expanding the government's provisions for enforcing copyright laws, SOPA would also make streaming copyrighted material a felony under U.S. law, punishable by up to five years in prison.

Where can I read the full text of the bill?
To learn more about SOPA, you can find the bill's full text online at OpenCongress.org.

What action can I take?
You can easily send your Congressperson a note with your thoughts on SOPA at AmericanCensorship.org.

Where can I watch SOPA online?
The second day of the hearing is over for now, but when the markup resumes, you can watch the House Judiciary Committee action live at Keepthewebopen.com or on the House's official website (we haven't been able to get that livestream to work, but maybe you'll have more luck!).

Wikipedia May Blackout All Articles To Protest SOPA

In protest against the highly-controversial ’Stop Online Piracy Act’ (SOPA), which will come up for a vote by the Senate s House Judiciary Committee later this week, Wikipedia may blackout all of its English-language articles. The proposal was issued by Wikipedia founder Jimmy Wales, who argued in support of the idea on his person Wikipedia user page after the Italian Wikipedia community achieved success with a similar protest. He has asked the online encyclopedia s users and editors to say whether or not they support such a blackout.

"A few months ago, the Italian Wikipedia community made a decision to blank all of Italian Wikipedia for a short period in order to protest a law which would infringe on their editorial independence. The Italian Parliament backed down immediately. As Wikipedians may or may not be aware, a much worse law going under the misleading title of ’Stop Online Piracy Act is working its way through Congress on a bit of a fast track," wrote Wales. "My own view is that a community strike was very powerful and successful in Italy and could be even more powerful in this case."

SOPA would allow corporations (i.e. copyright holders) and the US government to block access to websites that are suspected of spreading pirated material, or facilitate such activity. Supporters of SOPA say that the legislation is needed to further fight online piracy and protect copyright holders from intellectual property theft. The opposition movement against SOPA - a faction that includes an increasing number of tech heavyweights, like Google, Facebook, Twitter, AOL, eBay, Yahoo and even Microsoft (among many others) - insist that SOPA is dangerous because it could usher in unprecedented online censorship, and potentially jeopardize the entire underlying structure of the Internet (the Domain Name System, or DNS), thus making it less secure.

The Wikipedia straw poll is currently ongoing, and well worth the read, as each voter is able to write why he or she supports or opposes the Wikipedia blackout. Self-described hacker Shishir Bashyal has created a pie chart, automatically updated every two minutes, which currently shows that 88.5 percent of respondents support (55.4 percent) or strongly support (30.1 percent) the community strike. Only 14.6 percent currently oppose (10.4 percent) or strongly oppose (4.2 percent) the blackout.

Wales says that this straw poll will simply be used to gauge opinion on the matter, but will not itself decide whether the blackout will happen. But "if this poll is firmly in support ," writes Wales, "we d obviously go through a much longer process to get some kind of consensus around parameters, triggers, and timing."

U.S., Russia Work To Expand Cyberspace Cooperation

Russia and the United States are planning a regular exchange on "technical threats" that appear to come from computers in each other’s territories, a White House spokeswoman said on Friday, even as bilateral ties have come under growing strains.

A range of mechanisms aimed at confidence building and crisis prevention are being planned to cope with alarming events in cyberspace, said Caitlin Hayden, a spokeswoman for the White House National Security Council.

These include "regular exchanges on technical threats that appear to emanate from one another's territory" as well as "no-fail communications mechanisms to help prevent crisis escalation and build confidence," she said in an emailed reply to a query.

Some such links have existed for years, including the Nuclear Risk Reduction Center, but others are "cyber-specific and would begin working with Moscow for the first time," Hayden said, without giving a projected start date.

A representative of the Russian Embassy in Washington did not return a phone call seeking comment.

Vice President Joe Biden said last month the United States was working with Moscow to link computer emergency response teams and the nuclear risk reduction centers and setting up lines of communication in case of "an alarming incident."

"It's a great deal harder to assess another nation's cyber-capabilities than to count their tanks," he told the London Conference on Cyberspace on November 1 by videocast.

Howard Schmidt, the White House cybersecurity coordinator, said in a July 12 blog that the United States and Russia planned to have three types of cybersecurity-related cooperative mechanisms in place by the end of this month, including special "24/7" communications links.

Hayden, the spokeswoman, declined to spell out the status of the talks with Russia, referring only to "ongoing diplomatic discussions." No such links were being announced for now with China or any other country, she said.

Strains between Washington and Moscow over Russia's disputed parliamentary elections are threatening President Barack Obama's "reset" policy, and the two countries remain at odds over NATO missile defense plans in Europe.

In another sore point, a U.S. intelligence report to Congress in October said Russia's intelligence services "are conducting a range of activities to collect economic information and technology from U.S. targets."

"We judge that the governments of China and Russia will remain aggressive and capable collectors of sensitive U.S. economic information and technologies, particularly in cyberspace," the Office of the National Counterintelligence Executive, a U.S. intelligence arm, said.

Schmidt, in his blog, did not speak of any attempt to reduce the risk of spying but rather of heading off threats to both sides such as "botnets," a collection of computers that can be used to swamp a web site with incoming traffic or other malicious action.

Another goal, he said at the time, was to better understand each other's military view on operating in cyberspace.

"It's a prime example of the 'reset' in relations taking on a new and important dimension," Schmidt wrote then.

Jury Says Verdict Close in $1 Billion Microsoft Lawsuit

Jurors have resumed deliberations in a Utah company’s $1 billion federal antitrust lawsuit against Microsoft Corp. and say they’re close to a verdict.

Novell Inc. sued in 2004, claiming Microsoft duped it into developing a version of its WordPerfect writing program for Windows 95 only to pull the plug so Microsoft could gain market share with its own Word program.

Microsoft co-founder Bill Gates testified last month that Novell just couldn’t deliver a compatible WordPerfect program in time for the rollout, and that Microsoft’s own Word program was actually better.

Jurors said late Thursday they were making progress deciding whether Novell was entitled to damages. On Friday morning, they said they were close to finishing deliberations.

Facebook Aims To Help Prevent Suicide

Facebook is making it easier for people who express suicidal thoughts on the social networking site to get help.

A program launching Tuesday enables users to instantly connect with a crisis counselor through Facebook’s "chat" messaging system.

The service is the latest tool from Facebook aimed at improving safety on its site, which has more than 800 million users. Earlier this year, Facebook announced changes to how users report bullying, offensive content and fake profiles.

"One of the big goals here is to get the person in distress into the right help as soon as possible," Fred Wolens, public policy manager at Facebook, told The Associated Press.

Nearly 100 Americans die by suicide every day, and 36,035 a year, according to U.S Surgeon General Regina Benjamin’s office.

Google and Yahoo have long provided the phone number to the National Suicide Prevention Lifeline as the first result when someone searches for "suicide" using their sites. Through email, Facebook also directed users to the hotline or encouraged friends to call law enforcement if they perceived someone was about to do harm.

The new service goes a step further by enabling an instant chat session that experts say can make all the difference with someone seeking help.

"The science shows that people experience reductions in suicidal thinking when there is quick intervention," said Lidia Bernik, associate project director of Lifeline. "We’ve heard from many people who say they want to talk to someone but don’t want to call. Instant message is perfect for that."

Some crisis lines such as Lifeline have been criticized for alerting police without the caller or user knowing.

How the service works is if a friend spots a suicidal thought on someone’s page, he can report it to Facebook by clicking a link next to the comment.

Facebook then sends an email to the person who posted the suicidal comment encouraging them to call the hotline or click on a link to begin a confidential chat.

Facebook on its own doesn't troll the site for suicidal expressions, Wolens said. Logistically it would be far too difficult with so many users and so many comments that could be misinterpreted by a computer algorithm.

"The only people who will have a really good idea of what's going on is your friends, so we're encouraging them to speak up and giving them an easy and quick way to get help," Wolens said.

There have been high-profile incidents of suicidal expressions on Facebook.

Last month, authorities in California said a man posted a suicide note on Facebook before he killed his wife and in-laws then himself.

In July, police in Pennsylvania said they believed they were able to help prevent a man's suicide after the man's friend in California alerted police about a distraught Facebook posting. Police met with the man, who was committed to a hospital.

The Lifeline currently responds to dozens of users on Facebook each day. Crisis center workers will be available 24 hours a day to respond to users selecting the chat option.

Chrome 15 Takes Top Spot for Browsers

There's a new top dog among browser versions. Recent statistics show Google's latest Chrome browser has taken the No. 1 spot, bumping out the most popular version of Internet Explorer from Microsoft.

According to StatCounter.com data released Thursday, Chrome 15 now captures 24.55 percent of the world market, edging out IE8's 22.9 percent. Mozilla's Firefox 9.0 is at 14 percent, and IE9 is in fourth at 10.4 percent. Those rankings, covering the last half of November and the first week in December, are of particular release versions. \

When taken as a brand, with all versions combined, IE is still tops with 39.5 percent market share, Chrome is second at 26.5 percent, and Firefox takes a close third at 25.3 percent. As newer versions cycle in and older ones drop out, the brand rankings could begin to reflect the latest version rankings.

This is the first time since IE8 was released in early 2010 that it has not been in the top spot, and this is the first time any browser not developed by Microsoft has had the lead. In the U.S., IE8 still leads, at 27 percent for the week of December 5, compared with Chrome 15's 18.1 percent.

A key factor in the browser horse race appears to be the updating mechanism. Google released Chrome 16 Wednesday, which will automatically replace most users' Chrome 15 via the update mechanism. The auto-updating has been a feature of the browser since Chrome's introduction three years ago.

Mozilla has gotten some flak over its frequent update plan for Firefox, which involves user consent every six weeks to receive the latest incarnation. Firefox had previously had "silent updating," but that was dropped a year ago in favor of user notification and consent. Now, it will move back to automatic updating, expected to roll out in mid-2012.

"One of the negative side effects," wrote Mozilla developer Brian Bondy in October on his blog, "is that minor annoyances with software updates suddenly become much more noticeable. Most users don’t want to think about software updates nor version numbers and now they are being forced to do so every six weeks."

On his blog, Mozilla Foundation Chairman Mitchell Baker wrote earlier this fall that users were alerted to Firefox updates "to make sure people are aware and in control of what’s happening in their environment." But, he said, users are complaining of "update fatigue," because the "notifications are irritating."

The frequent updating has reportedly led to users of various browsers having to update browser-based apps on some cycle as well. But auto-upgrades are feeding the browser race, and Microsoft said Thursday it will start auto-upgrading IE in January, for users who have opted for auto-updates. Enterprises will still be able to control updates.

Previously, Microsoft had requested permission before updating, but now users will automatically receive the latest version available for that operating system version. The auto-updating for IE will start in Australia and Brazil first, and then roll out to other markets on a schedule to be announced.

Automatic Updates Coming To Internet Explorer

Microsoft intends to begin delivering automatic updates of its Internet Explorer browser beginning next year to ensure that as many machines as possible running Windows XP, Vista and Windows 7 are protected from the latest malware schemes of cyber criminals.

"Automatic updates are a very good idea based on every piece of security research I’ve seen," said White Hat Security CTO Jeremiah Grossman. "Keeping software up to date - particularly Web browsers - is critical for online security."

The new service will be available initially to those Windows customers who have activated the automatic update feature in Windows. The plan is to introduce automatic IE upgrades gradually - with the first Windows users to see the new offering located overseas and then scaling up delivery over time.

"This is an important step in helping to move the Web forward," noted Ryan Gavin, the general manager of Internet Explorer business and marketing at Microsoft.

"We will start in January for customers in Australia and Brazil who have turned on automatic updating via Windows Update," he wrote in a blog Thursday.

According to Microsoft’s latest security intelligence report, the biggest online threat that Windows users face comes from socially engineered malware targeting outdated Web browsers and other aging software. Making the move to the most current products and services helps PC users increase their protection against the most prevalent online threats, the software giant said.

One of the popular features of Google’s Chrome Web browser has long been its seamless, out-of-sight upgrades under the hood. Earlier this year, Mozilla likewise indicated that it would emulate Google’s browser upgrade strategy by early 2012 and now Microsoft intends to follow suit.

On desktop PCs, notebooks and netbooks, IE currently holds a 52.6 percent share of the global browser market - down from 58.8 percent in December of 2010, according to Net Applications. By adding automatic updates, however, Microsoft stands a better chance of hanging on to the IE users it already had locked in.

"I do think it will affect the rates at which people change browsers - mainly because I think people consider switching when they are going through an upgrade cycle," said Net Applications Executive Vice President Vincent Vizzaccaro. "If the upgrade cycle happens in the background, that will take away that reminder to consider switching browsers."

Large corporations, educational institutions and other organizations which need time to evaluate and fully integrate the latest browser upgrades will have the ability to opt out of the automatic upgrade program and develop customized browser upgrade schedules that best fit their respective business requirements.

"The Internet Explorer 8 and Internet Explorer 9 Automatic Update Blocker toolkits prevent automatic upgrades of IE for Windows customers who do not want them," Gavin wrote.

Individual consumers with automatic updating via Windows Update switched on will retain the same personal home page, search provider and default browser settings after receiving each new browser upgrade. Additionally, consumers who have previously declined invitations to install IE8 or IE9 on their PCs will not be forced to do so.

"Future versions of IE [also] will provide an option in the product for consumers to opt out of automatic upgrading," Gavin said.

Individual IE users also will be able to uninstall any IE browser update and continue receiving support for the specific version of IE that they prefer to run on their machines. Still, Gavin noted that "the Web overall is better - and safer - when more people run the most up-to-date browser."

Chrome Is The Most Secured Browser

Google Chrome offers more protection against online attacks than any other mainstream browser, according to an evaluation that compares exploit mitigations, malicious link detection, and other safety features offered in Chrome, Internet Explorer, and Firefox.

The 102-page report, prepared by researchers from security firm Accuvant, started with the premise that buffer overflow bugs and other

security vulnerabilities were inevitable in any complex piece of software. Rather than relying on metrics such as the number of flaws fixed or the amount of time it took to release updates, the authors examined the practical effect protections included by default in each browser had on a wide class of exploits.

Their conclusion: Chrome is the most secured browser, followed closely by Microsoft IE. Mozilla's open-source Firefox came in third, largely because of its omission of a security sandbox that shields vital parts of the Windows operating system from functions that parse JavaScript, images and other web content.

"We found that Google Chrome did the most sandboxing," Chris Valasek, who is a senior research scientist for Accuvant, told The Register. "It restricted the movements more than any other browser. Internet Explorer came up a close second because it implemented a sandbox where you could do certain things but you were allowed to do more things than you could in Chrome. Lastly, Firefox came in last because it didn't implement a sandbox yet."

The report was commissioned by Google, but the authors insist they had complete autonomy in deciding what metrics to use and what conclusions they made. The researchers have released more than 20MB worth of data, software tools, and methodology so peers may review or build upon the research. The study focused solely on the security offered by Chrome, IE, and Firefox, which when combined account for more than 93 percent of web users, according to the report. All three browsers tested were run on Windows 7.

Their finding is backed up by anecdotal evidence, as well. Chrome has emerged unscathed during the annual Pwn2Own hacker contest for three years in a row, something no other browser entered has done. Reports of in-the-wild exploits that target the browser are also extremely rare.

In much the way traditional sandboxes prevent sand from mixing with grass on a playground, security sandboxes isolate application code inside a perimeter that's confined from sensitive OS functions. By placing severe restrictions on an application's ability to read and write to the hard drive and interact with other peripheral resources, sandboxes are designed to lessen the damage attackers can do when they successfully exploit a vulnerability in the underlying code base.

The so-called token in the Chrome sandbox, for instance, doesn't allow browser processes to access files outside of an extremely limited set of directories. It also forbids them from creating connections known as network sockets to communicate directly with servers over the internet. The sandbox in IE, by contrast, allows browser resources to read almost all parts of a hard drive and puts few restrictions on the creation of network sockets, the researchers said.

As a result, attackers who exploit a vulnerability in the Microsoft browser will have an easier time accessing contacts, documents, and other data stored on the hard drive of a targeted computer and uploading it to a command and control server.

"The Google Chrome token is far more restrictive," said Accuvant Chief Research Scientist Ryan Smith, who compared tokens to a driver's license that spells out what vehicles a holder is permitted to drive and other conditions, such as whether eyeglasses are required. "It's more like a

learner’s permit, whereas the Internet Explorer token is more like a Class C regular driver’s license."

The researchers analyzed each browser’s ability to read files, write files, and perform 13 other actions. As indicated in the graphic below, Chrome blocked all but two of them. Of those, one known as "system parameters" was partially blocked. IE, meanwhile, completely blocked only two actions, and partially blocked seven more actions. Seven additional actions, including the ability to read files, access networks, and create processes, were completely unrestricted.

In last place was Firefox, which allowed nine actions and partially blocked the remaining six actions.

The report refers to sandboxing as a "standard best practice within many popular applications." Chrome implements sandboxes in versions that run on Windows, MacOS X, and Linux. Microsoft deployed sandboxing more than five years ago, starting when users ran IE version 7 on Windows Vista or later versions of Windows. Even Apple, which commands a tiny fraction of the browser market, implemented a robust sandbox in versions of Safari that run on Lion, the latest release of OS X.

In this context, the continuing failure of Firefox to offer sandboxing features is hard to excuse.

In a statement issued prior to the release of Accuvant’s report, Johnathan Nightingale, Mozilla’s director of Firefox engineering, said:

"Firefox includes a broad array of technologies to eliminate or reduce security threats, from platform level features like address space randomization to internal systems like our layout frame poisoning system. Sandboxing is a useful addition to that toolbox that we are investigating, but no technology is a silver bullet. We invest in security throughout the development process with internal and external code reviews, constant testing and analysis of running code, and rapid response to security issues when they emerge. We’re proud of our reputation on security, and it remains a central priority for Firefox.

The researchers also gave Chrome high marks for the strict limitations it places on software add-ons that extend the things users can do with the browser. As a result, attackers who manage to exploit extension bugs or trick victims into installing malicious add-ons are severely limited in the damage they can do. By comparison, IE and Firefox give extensions much wider latitude. IE add-ons, for instance, have the ability to create processes and to access the Windows clipboard, which can be a means of funneling malicious data from one application to another.

The other area where Chrome outflanked its rivals was its offering of what’s known as JIT hardening. Short for just in time, JIT refers to code that’s compiled on the fly and executed inside the browser. Attackers have long relied on JIT techniques to convert JavaScript into malicious machine code that bypasses exploit mitigations such as ASLR.

JIT hardening in Chrome, and to a lesser extent in IE, counteract JIT attacks by compiling JavaScript in an unpredictable way that makes it hard for attackers to control. Mozilla developers have yet to implement the feature in Firefox.

Besides ranking the security of the top three browsers, the paper argues that many of the metrics regularly used to gauge how well software

stands up to hack attacks are unreliable. One such metric is the number of vulnerabilities patched, based on the assumption that more bugs indicate poorer-quality code than programs with fewer bugs. Other frequently cited factors include how quickly bugs are fixed and the severity of the bugs.

In the end, a browser will either succumb to a given exploit or it won't, and that's all that mattered to the paper's authors.

"We really didn't believe those [metrics] had much merit because it's really hard to correlate those things, especially between browsers and vendors," said Valasek, who along with Smith, was assisted by Accuvant colleagues Joshua Drake, Paul Mehta, Charlie Miller, and Shawn Moyer. "So we decided: Let's focus this paper on exploitation mitigation technology to show how these actually stand up against attackers when they find a vulnerability."

HP To Contribute webOS to Open Source

HP today announced it will contribute the webOS software to the open source community.

HP plans to continue to be active in the development and support of webOS. By combining the innovative webOS platform with the development power of the open source community, there is the opportunity to significantly improve applications and web services for the next generation of devices.

webOS offers a number of benefits to the entire ecosystem of web applications. For developers, applications can be easily built using standard web technologies. In addition, its single integrated stack offers multiplatform portability. For device manufacturers, it provides a single web-centric platform to run across multiple devices. As a result, the end user benefits from a fast, immersive user experience.

"webOS is the only platform designed from the ground up to be mobile, cloud-connected and scalable," said Meg Whitman, HP president and chief executive officer. "By contributing this innovation, HP unleashes the creativity of the open source community to advance a new generation of applications and devices."

HP will make the underlying code of webOS available under an open source license. Developers, partners, HP engineers and other hardware manufacturers can deliver ongoing enhancements and new versions into the marketplace.

HP will engage the open source community to help define the charter of the open source project under a set of operating principles:

- The goal of the project is to accelerate the open development of the webOS platform
- HP will be an active participant and investor in the project
- Good, transparent and inclusive governance to avoid fragmentation
- Software will be provided as a pure open source project

HP also will contribute ENYO, the application framework for webOS, to the community in the near future along with a plan for the remaining components of the user space.

Beginning today (Tuesday), developers and customers are invited to provide input and suggestions at http://developer.palm.com/blog/.

Most People Still Don’t Trust Online Info

Over the past decade, Americans have witnessed the rise of social networks and mobile technology that’s put the Internet at an arm’s reach, day and night - yet a new study has found that people are even more distrustful of the information they find online.

Three-quarters of Internet users find the Web an important source of information, but most people still don’t deem the content they see online reliable, according to a report out this week from the University of Southern California.

Such are the deep chasms among Americans’ attitudes about the Internet.

In 2010, 15 percent of Internet users said they find only a small portion of online information reliable. That’s greater than the 7 percent who were likewise skeptical of the vast majority of information they come across on the Internet.

The mistrust is especially true for social networks. That said, people don’t look to social networks for reliability. Rather, they visit the sites to socialize and share photos, updates and videos.

Trust grows when it comes to established media outlets and government websites. In 2010, 79 percent of Internet users said they found content posted on government websites reliable, about the same as in 2003, the first year the center looked at that question.

Jeff Cole, author of the study and director of USC Annenberg School’s Center for the Digital Future, said Americans tend to be more trusting of government and big media.

"Other countries are better at distinguishing good information from (the) unreliable," he said. In repressive regimes where media is closely tied to the government, citizens grow adept at filtering truth from propaganda.

When it comes to privacy online, Americans are actually more concerned about businesses than the government, the report found. Nearly half of U.S. Internet users said they are worried about companies watching what they do online, compared with 38 percent who said the same for the government.

Looking ahead to the next decade, Cole expects tablet computers and other touch-screen devices to largely replace personal computers and with them, the clunky computer mouse.

The center has surveyed more than 2,000 U.S. households each year since 1999. The latest report is a look back at the past decade of Americans’ Internet use. The margin of error is plus or minus 3 percentage points.

Consumers Not Turning to Social Media Sites for Local Business Info

People who look for information about local restaurants and businesses are turning to the Internet but not social media sites, according to a new study.

The Pew Internet and American Life Project found that the Internet far outpaces other sources for local business information, followed by newspapers and word of mouth. Yet people rely very little on sites such as Facebook and Twitter for this type of information.

More than half (51%) of adults who look for news and information about local restaurants, bars and clubs use the Internet to do so. About 38% of this demographic performs search engine queries for local restaurant information, while 17% visit specialty sites. Only 3% said they turn to social networking sites.

Even more surprising is that only one percent of those who look for information about local businesses beyond restaurants - such as retail stores - turn to social networking sites. The news comes as more local restaurants and businesses focus marketing initiatives around social media sites.

Small businesses aren’t convinced about the impact of social media either. A study revealed last month that only 12% of local businesses considered using social media a "must" for their business, while 50% said they couldn t do without word-of-mouth marketing.

Meanwhile, the more recent Pew report found that newspapers remain popular for finding out information about local businesses. Among the 31% of culture seekers who prefer this method, about 26% read printed copies while 5% visit their favorite newspaper sites. Word of mouth is also a popular way to find out information about local spots, with 23% of respondents who look for business information reporting that as their favored approach.

People who seek out information and news about local businesses and restaurants are more likely to have college educations and earn a salary of $75,000, according to Pew. This group is also more likely to be young female adults living in urban environments.

The study was conducted over the phone among 2,251 adults age 18 and older, with a margin of error of 2.4%.

Are you surprised that more people aren’t turning to social media sites for local business information? What can local businesses do to make its social networking profiles more of a destination for information?

Twitter Stalking Is Protected Free Speech, Judge Rules

A San Francisco judge has declared cyberstalking on Twitter and blogs constitutionally-protected free speech, reports The New York Times. The ruling is a victory for the First Amendment. But like all things worth fighting for, it comes at a price.

Here s what happened: A Buddhist religious leader in Maryland named Alyce Zeoli became friends with a man named William Lawrence Cassidy. At some

point, the two had a falling out. Cassidy took the mature route, and began posting thousands of messages on blogs and Twitter, often using pseudonyms, that aggressively disparaged Zeoli. Some of them even called for her death.

Understandably distraught, Zeoli then worked with the FBI to have Cassidy arrested, which he was, based on interstate stalking laws. Cassidy, the government argued, had caused Zeoli "substantial emotional distress."

This, however, was not enough to convince Judge Roger W. Titus, who declared that Cassidy s actions, while distasteful, were not enough to set a precedent that could cause serious harm to the entire foundations of speech on the Internet.

"[W]hile Mr. Cassidy s speech may have inflicted substantial emotional distress, the government s indictment here is directed squarely at protected speech: anonymous, uncomfortable Internet speech addressing religious matters," wrote Judge Titus, in his official order.

Titus ruled that, because no one was forced to read Cassidy s posts and tweets - as opposed to a "telephone call, letter or email specifically addressed to and directed at another person" - they are considered free speech, not harassment, just as personal bulletin boards of the colonial era fell under the protection of the First Amendment, which "protects speech even when the subject or the manner of expression is uncomfortable and challenges conventional religious beliefs, political attitudes or standards of good taste."

One of Zeoli s lawyers, Shanlon Wu, told the Times that Zeoli was "appalled and frightened by the judge s ruling." It is not yet clear whether there will be an appeal to the ruling.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.